THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF THE RESIDENCE AT 819 EAST GUINEVERE STREET SPRINGFIELD, MISSOURI 65807

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, James D. Holdman Jr., being first duly sworn, do hereby depose and state that:

1. This affiant is a Special Agent (SA) with United States Immigration and Customs Enforcement (ICE) Office of Homeland Security Investigations (HSI) in Springfield, Missouri. This affiant has been employed with ICE/HSI since June of 2003. This affiant has been employed in the field of law enforcement since January 1989, including duties as a deputy sheriff in Washington County, Missouri, and a criminal investigator for the State of Missouri.

2. As part of this affiant's duties with ICE/HSI, this affiant investigates criminal violations relating to child exploitation, child pornography, human trafficking, and coercion and enticement, in violation of 18 U.S.C. §§ 2251, 2422(a) and (b), 2252(a), and 2252A. This affiant has received training in the areas of child pornography, child exploitation and human/sex trafficking,

3. This affiant has conducted operations relating to the exploitation of children and adults in Costa Rica, the border area of the United States and Mexico, and the Philippines. This affiant has instructed classes on sexual exploitation of children, interviewing, evidence collection, case studies, and undercover operations to law enforcement agencies within the United States, including five national conferences, as well as to law enforcement located in the following foreign countries:

a. National Police Academy in Phnom Penh and Siem Reap, Cambodia;

b. International Law Enforcement Academy (ILEA) in El Salvador;

c. National Police Academy in Kenitra, Morocco;

d. Ontario Provincial Police in Niagara Falls, Canada; and

e. Royal Canadian Mounted Police Headquarters in Ottawa, Canada.

4. The statements in this affidavit are based on personal observations, training and experience, investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to me concerning this investigation. This affiant has set forth the facts necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, and 2252A are currently located at 819 East Guinevere Street, Springfield, Missouri 65807, which is located in the Western District of Missouri.

5. This affidavit is in support of an application for a search warrant for evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing possession, receipt, distribution, and production of child pornography. The property to be searched is described in the following paragraphs and in Attachment A. This affiant requests the authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.

6. This affiant has probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, involving the use of a computer in or affecting interstate commerce to receive, distribute, possess, and produce child pornography, is located in

and within the aforementioned property described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the aforementioned crimes are located in this property.

STATUTORY AUTHORITY

7. This investigation concerns alleged violations of Title 18, United States Code, §§ 2251, 2252, and 2252A, relating to material involving the sexual exploitation of minors:

a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.

b. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

c. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. §2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography

was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

8. The following definitions apply to this Affidavit and its Attachments:

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "sexually explicit conduct," 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

e. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical,

or other means, of sexually explicit conduct, where:

1. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, and painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to, phonograph records, printing, and typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet.

ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

h. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

i. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

j. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

9. Based on this affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this affiant has had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced

and distributed.

10. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

11. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

12. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

13. The Internet affords individuals several different venues for meeting on another, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

14. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

15. As with most digital technology, communications made from a computer are often saved

or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only

overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

CELLULAR PHONES AND CHILD PORNOGRAPHY

16. Based on this affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this affiant has had discussions, cellular phones have likewise revolutionized the manner in which child pornography is produced and distributed.

17. Cellular phones ("cell phones") are exceptionally widespread. The Central Intelligence Agency estimates that in 2009 there were 286 million cell phone subscribers in the United States. Cell phones increasingly offer features such as integrated digital cameras, the ability to store hundreds of digital images, and the ability to access and browse the Internet.

18. In this affiant's training and experience, the ready availability and personal nature of cell phones has led to their frequent use in the commission of child pornography offenses. Individuals with a sexual interest in children will often use their cell phone to browse the Internet and to distribute, receive, and store child pornography files. Individuals producing child pornography will also frequently use the integrated digital camera within a cell phone to produce the images, and then store the images both on the phone and on other devices – such as computers and computer storage media.

19. Cell phones, like other computer systems, will frequently retain data relating to activities, such as Internet browsing history, digital images, and other digital data, that can remain

stored for a long period of time.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND CELL PHONES

20. Searches and seizures of evidence from computers and cell phones commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and are generally difficult to accomplish fully on-site.

b. Searching computer systems and cell phones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased,

compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

21. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

22. Furthermore, because there is probable cause to believe that the computer, its storage devices and cell phones are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

BACKGROUND OF INVESTIGATION

23. On March 9, 2017, agents from HSI in Syracuse, New York, assisted the New York State Police (NYSP) Computer Crimes Unit (CCU) Troop D with a child exploitation investigation. During the course of the investigation, David G. Hullihen was arrested for three counts of promoting a sexual performance of a child, in violation of New York State Penal Law, PL 263:15. Hullihen provided consent for the investigators to assume control of his Kik account, having the username, "hotfamilyfun1," designated hereinafter as the "UC account."

24. On March 13, 2017, at 10:50 AM ET, agents noted that the UC account was a member of

a chat group called "Little (G or B) Links," with chat identification number "pth666." This chat group appeared to be very active, with a full 50-member capacity. Members of the chat group were observed uploading images and videos containing depictions of child pornography, along with links to Dropbox and pcloud accounts. NYSP CCU recorded this chat session and captured the child pornography uploads and chat dialogue.

25. On March 20, 2017, investigators attempted to access the UC account to observe the chat group, but discovered that the UC account had been deactivated. The investigators were, however, able to review communications that occurred on the "Little (G or B) Links" group on March 16, 2017.

26. During the recorded chat sessions, a Kik user, identified as "LostnHungry," was identified as a group chat administrator, denoted by the orange crown icon on his user account. During the recorded session, "LostnHungry" appeared to be actively monitoring other users and warning them to follow the rules of the chat group.

27. The list of rules for the "Little (G or B) Links" chat group are as follows: (1) Post on entry (vid or link); (2) Don't request anything without posting additional material (even if you posted already); (3) ASK before PMing; (4) You must have a profile pic; (5) Only admins can invite people; (6) We do not accept lurkers; (7) Limits none, just post young for first post(12-down); (8) People inactive for two days will be removed; and (9) Don't complain.

28. During the session, "LostnHungry" actively encouraged other users to post child pornography and removed members from the chat group for failing to abide by the rules. "LostnHungry" reminded members of the rules repeatedly, specifically posting rules 1, 4, and 7.

29. In one such instance, in the recorded Kik chat session titled "Kik chat March 16 prior to being removed," "LostnHungry" states "mr right, you need to post 12-for your first post...not 16+..."

30. In the recorded Kik chat session entitled "Kik log in and monitored chat groups 3/13/2017," "LostnHungry" posted the following messages to the group: (1) "Erica, you need to post or I'll have to remove you;" (2) "Alex you'll need to post if you want to stay also you need a profile pic to be in this group;" (3) "you will need to follow the rules if you want to stay;" and (4) "post and have a profile pic or I'll have to remove you."

31. During another recorded chat session, "LostnHungry" posted several video files to the chat room. The investigators were able to determine that IP address 107.210.103.65 was utilized to upload the files. The files are described below:

    a. The first video file depicts a nude minor female inserting an object into her vagina.

    b. The second video file depicts a nude prepubescent female lying on her back with legs spread apart exposing her vagina in a lewd and lascivious manner.

    c. The third video file depicts a nude prepubescent female performing oral sex on an erect penis.

32. During the chat session that the videos were posted, "LostnHungry" encouraged others to post similar videos. Specifically, "LostnHungry" posted the statement, "Missy, if you feel like sharing some more of your daughter, the group would really like it."

33. On March 22, 2017, HSI SA Lon Ziankoski issued a subpoena to Kik interactive for subscriber information relating to Kik user "LostnHungry."

34. On March 24, 2017, Kik provided the following information pertaining to the user

identified as "LostnHungry:"

a. First Name: Nick;

b. Last Name: Y;

c. email of York.nick@yandex.com;

d. Username: LostnHungry;

e. Device type: Android; and

f. Country code: United States.

35. On June 19, 2017, SA Ziankoski sent a subpoena to AT&T Internet Services for subscriber information in reference to IP address 107.210.103.65 for login dates between March 13, 2017, 21:18:52 UTC and March 16, 2017, 22:40:01 UTC.

36. On June 26, 2017, AT&T Internet Services responded to the subpoena and provided the following subscriber information: Account name: Anthony Cotter; Contact name: Heather Cotter; phone numbers 417-450-0994 and 417-619-5547; email address: heather.cotter@gmail.com and heathrely84@att.net; and account established February 5, 2013, with service address of 819 East Guinevere, Springfield, Missouri 65807.

37. On June 21, 2017, this affiant reviewed the recorded chats mentioned in this affidavit and information supplied by SA Ziankoski of the chat group with the administrator "LostnHungry." It was clearly evident to this affiant that members of the chat group were receiving and distributing images and videos of child pornography. This affiant reviewed videos and images files depicting children, ranging from infants to approximately 12 years old. The images and videos depicted various types of sexual abuse to the children perpetrated by adult males and adult females including, but not limited to oral sex and vaginal and anal penetration. Some of the images/videos depicted

bondage and bestiality involving the sexual abuse of children under the age of 12.

38. One such posting depicted a juvenile female, about six to eight years old, having her vagina licked by a dog.

39. Another image depicts a nude juvenile female, approximately four to eight years old, lying face down on a couch, with her legs tied, exposing her vaginal and anal area. The juvenile child has her hands tied behind her back.

40. SA Ziankoski conducted database queries for Heather Michelle Cotter, revealing a date of birth of January 1, 1984, assigned social security number 551-91-6855, an address of 819 East Guinevere Street, Springfield, Missouri 65807, and phone numbers 417-450-0994 and 417-619-5547.

41. On July 7, 2017, this affiant conducted record checks which document Heather M. Cotter as a customer of city utilities at 819 East Guinevere Street, Springfield, Missorui 65807, with a year of birth of 1984.

42. On July 21, 2017, TFO Brian Martin contacted this affiant in reference to multiple cyber tips received from the National Center for Missing and Exploited Children (NCMEC). TFO Martin received cyber tips 21849797, 21849813, 21849816, 21849817, 21849819, and 21849820. The cyber tips were in reference to a Skype account being using to distribute images/videos of child pornography. Skype is an application that provides video chat and voice call services. The IP address used to distribute the images depicting child pornography was 107.210.103.65. The screen user name was identified as "live:thousandandonenights1001."

43. Cyber tip 21849797, received by NCMEC on June 27, 2017, was in reference to the transmission of an image depicting child pornography on June 26, 2017, at 20:13:40

hours CDT. TFO Martin viewed the image and reported that the image depicted an erect penis in front of the mouth of a female no older than four or five years old.

44. Cyber tip 21849813, received by NCMEC on June 27, 2017, was in reference to the transmission of an image depicting child pornography on June 26, 2017, at 20:13:45 hours CDT. TFO Martin viewed the image and reported that the image depicts an erect penis in the mouth of a child who appeared to be younger than five years old.

45. Cyber tip 21849816, received by NCMEC on June 27, 2017, was in reference to the transmission of an image depicting child pornography on June 26, 2017, at 20:13:45 hours CDT. The transmission involved the same image contained in Cyber tip 21849813.

46. Cyber tip 21849817, received by NCMEC on June 27, 2017, was in reference to the transmission of an image depicting child pornography on June 26, 2017, at 20:13:45 hours. TFO Martin viewed the image and reported that the image depicts a prepubescent female, topless, with an erect penis in her mouth.

47. Cyber tip 21849819, received by NCMEC on June 27, 2017, was in reference to the transmission of an image depicting child pornography on June 26, 2017, at 20:13:47 hours CDT. TFO Martin viewed the image and reported that the image depicted a child, younger than five years old, with an erect penis in her mouth.

48. Cyber tip 21849820, received by NCMEC on June 27, 2017, was in reference to the transmission of an image depicting child pornography on June 26, 2017, at 20:13:47 CDT. TFO Martin describes the image as the same juvenile female from cyber tip 21849817. The juvenile female has an adult's penis in her mouth.

49. TFO Martin told this affiant that, on July 21, 2017, he received a response to an investigative subpoena issued to AT&T for IP address 107.210.103.65. The subscriber

information identified Anthony and Heather Cotter, residing at 819 East Guinevere Street, Springfield, Missouri 65807, as the account holder. The email address for the account is heather.cotter@gmail.com, and the phone number associated with the account is 417-450-0994.

PROBABLE CAUSE

50. Based on the above facts, this affiant believes probable cause exists for the issuance of a warrant to search the premises described more fully in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means of committing a criminal offense, namely possible violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, including but not limited to the items listed in Attachment B.

James D. Holdman, Jr.
Special Agent
Homeland Security Investigations

Subscribed and sworn before me this 27th day of September, 2017.

David P. Rush
United States Magistrate Judge
Western District of Missouri